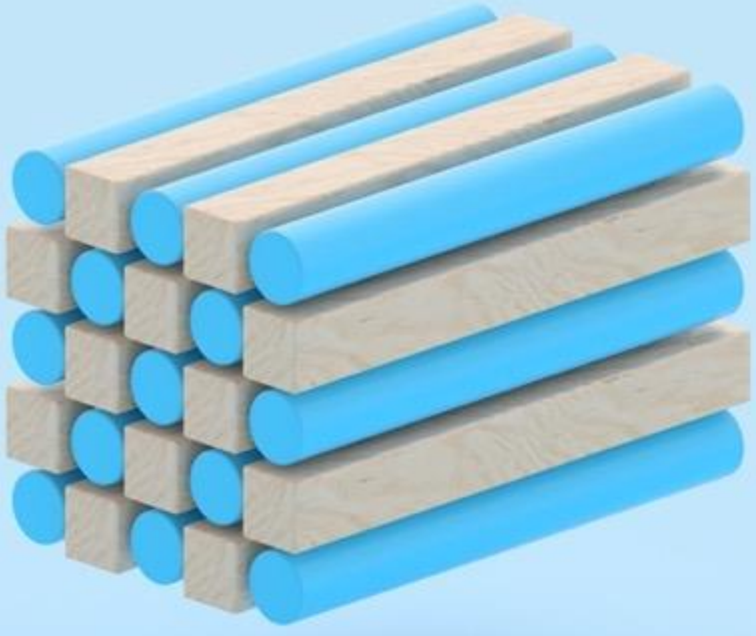
NetApp
安全資料堡壘 擺脫威脅攻擊

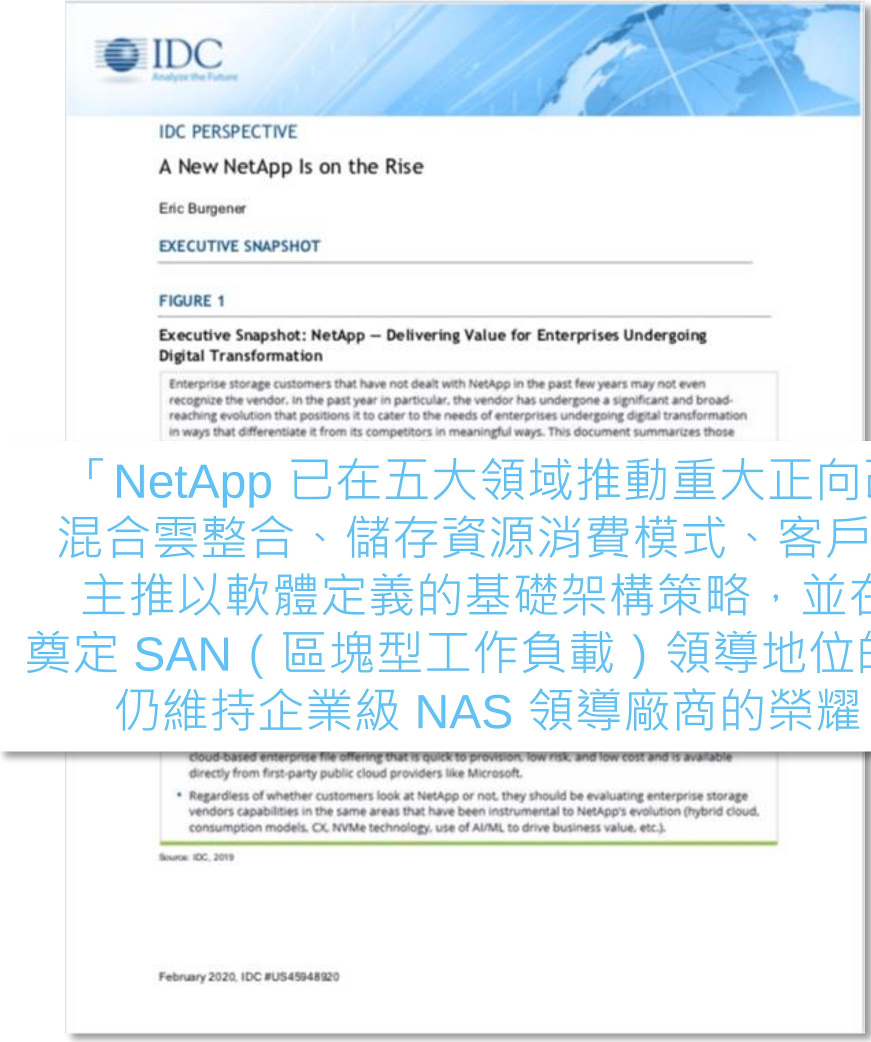
NetApp Help You to Secure Data & Fight Ransomware

NetApp



Major Chuang
Sr. Solutions Engineer
Sep 2022

IDC 觀點：嶄新 NetApp 正在崛起



IDC
Analyze the Future

IDC PERSPECTIVE

A New NetApp Is on the Rise

Eric Burgener

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: NetApp — Delivering Value for Enterprises Undergoing Digital Transformation

Enterprise storage customers that have not dealt with NetApp in the past few years may not even recognize the vendor. In the past year in particular, the vendor has undergone a significant and broad-reaching evolution that positions it to cater to the needs of enterprises undergoing digital transformation in ways that differentiate it from its competitors in meaningful ways. This document summarizes those

cloud-based enterprise file offering that is quick to provision, low risk, and low cost and is available directly from first-party public cloud providers like Microsoft.

- Regardless of whether customers look at NetApp or not, they should be evaluating enterprise storage vendors capabilities in the same areas that have been instrumental to NetApp's evolution (hybrid cloud, consumption models, CX, NVMe technology, use of AI/ML to drive business value, etc.).

Source: IDC, 2019

February 2020, IDC #US45948920

> 「NetApp 已在五大領域推動重大正向改革：混合雲整合、儲存資源消費模式、客戶體驗、主推以軟體定義的基礎架構策略，並在紮根奠定 SAN（區塊型工作負載）領導地位的同時，仍維持企業級 NAS 領導廠商的榮耀。」

資料來源：IDC，嶄新 NetApp 正在崛起，2020 年 2 月，Eric Burgener，#US45948920

您可能還不認識今日的 NetApp：

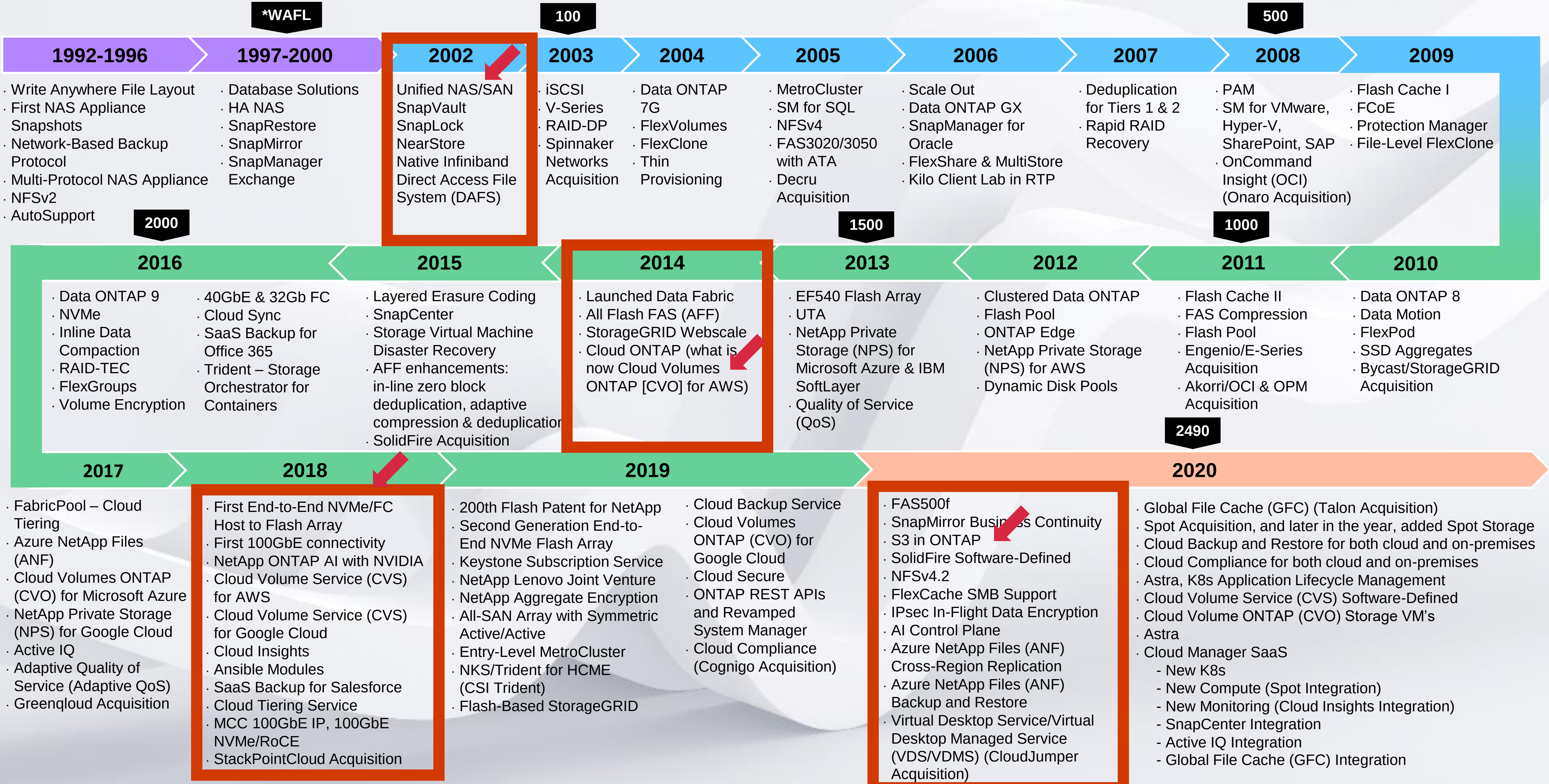
1. 既有儲存設備供應商中最先理解混合雲革新的重要性，並自此之後在本領域中保有領導地位的廠商。
2. 產品與銷售策略皆有重大改變，無論客戶是要購買內部部署或公有雲上的基礎架構資源，該公司都能順利因應未知需求。
3. 投注大量資源提升能力，能夠在整個客戶群中提供一致且優異的客戶體驗 (CX)。
4. 此時此刻，NetApp 更像是軟體公司，而非硬體設備廠商。
5. **NetApp 不應只被當成 NAS 廠商**。

如需完整報告，請按此處

NetApp: 30 Years of Customer-Focused Innovation

⬛ cumulative patents

*1998 first “Write Anywhere File Layout (WAFL)” patent awarded to Hitz, Malcom, Lau, and Rakitzis



1992-1996
- Write Anywhere File Layout
- First NAS Appliance
- Snapshots
- Network-Based Backup Protocol
- Multi-Protocol NAS Appliance
- NFSv2
- AutoSupport

*WAFL

1997-2000
- Database Solutions
- HA NAS
- SnapRestore
- SnapMirror
- SnapManager Exchange

2002
Unified NAS/SAN
SnapVault
SnapLock
NearStore
Native Infiniband
Direct Access File System (DAFS)

100

2003
- iSCSI
- V-Series
- RAID-DP
- Spinnaker Networks Acquisition

2004
- Data ONTAP 7G
- FlexVolumes
- FlexClone
- Thin Provisioning

2005
- MetroCluster
- SM for SQL
- NFSv4
- FAS3020/3050 with ATA
- Decru Acquisition

2006
- Scale Out
- Data ONTAP GX
- SnapManager for Oracle
- FlexShare & MultiStore
- Kilo Client Lab in RTP

2007
- Deduplication for Tiers 1 & 2
- Rapid RAID Recovery

500

2008
- PAM
- SM for VMware, Hyper-V, SharePoint, SAP
- OnCommand Insight (OCI) (Onaro Acquisition)

2009
- Flash Cache I
- FCoE
- Protection Manager
- File-Level FlexClone

2010
- Data ONTAP 8
- Data Motion
- FlexPod
- SSD Aggregates
- Bycast/StorageGRID Acquisition

1000

2011
- Flash Cache II
- FAS Compression
- Flash Pool
- Engenio/E-Series Acquisition
- Akorri/OCI & OPM Acquisition

2012
- Clustered Data ONTAP
- Flash Pool
- ONTAP Edge
- NetApp Private Storage (NPS) for AWS
- Dynamic Disk Pools

1500

2013
- EF540 Flash Array
- UTA
- NetApp Private Storage (NPS) for Microsoft Azure & IBM SoftLayer
- Quality of Service (QoS)

2014
- Launched Data Fabric
- All Flash FAS (AFF)
- StorageGRID Webscale
- Cloud ONTAP (what is now Cloud Volumes ONTAP [CVO] for AWS)

2015
- 40GbE & 32Gb FC
- Cloud Sync
- SaaS Backup for Office 365
- Trident – Storage Orchestrator for Containers
- Layered Erasure Coding
- SnapCenter
- Storage Virtual Machine Disaster Recovery
- AFF enhancements: in-line zero block deduplication, adaptive compression & deduplication
- SolidFire Acquisition

2000

2016
- Data ONTAP 9
- NVMe
- Inline Data Compaction
- RAID-TEC
- FlexGroups
- Volume Encryption

2017
- FabricPool – Cloud Tiering
- Azure NetApp Files (ANF)
- Cloud Volumes ONTAP (CVO) for Microsoft Azure
- NetApp Private Storage (NPS) for Google Cloud
- Active IQ
- Adaptive Quality of Service (Adaptive QoS)
- Greenqloud Acquisition

2018
- First End-to-End NVMe/FC Host to Flash Array
- First 100GbE connectivity
- NetApp ONTAP AI with NVIDIA
- Cloud Volume Service (CVS) for AWS
- Cloud Volume Service (CVS) for Google Cloud
- Cloud Insights
- Ansible Modules
- SaaS Backup for Salesforce
- Cloud Tiering Service
- MCC 100GbE IP, 100GbE NVMe/RoCE
- StackPointCloud Acquisition

2019
- 200th Flash Patent for NetApp
- Second Generation End-to-End NVMe Flash Array
- Keystone Subscription Service
- NetApp Lenovo Joint Venture
- NetApp Aggregate Encryption
- All-SAN Array with Symmetric Active/Active
- Entry-Level MetroCluster
- NKS/Trident for HCME (CSI Trident)
- Flash-Based StorageGRID
- Cloud Backup Service
- Cloud Volumes ONTAP (CVO) for Google Cloud
- Cloud Secure
- ONTAP REST APIs and Revamped System Manager
- Cloud Compliance (Cognigo Acquisition)

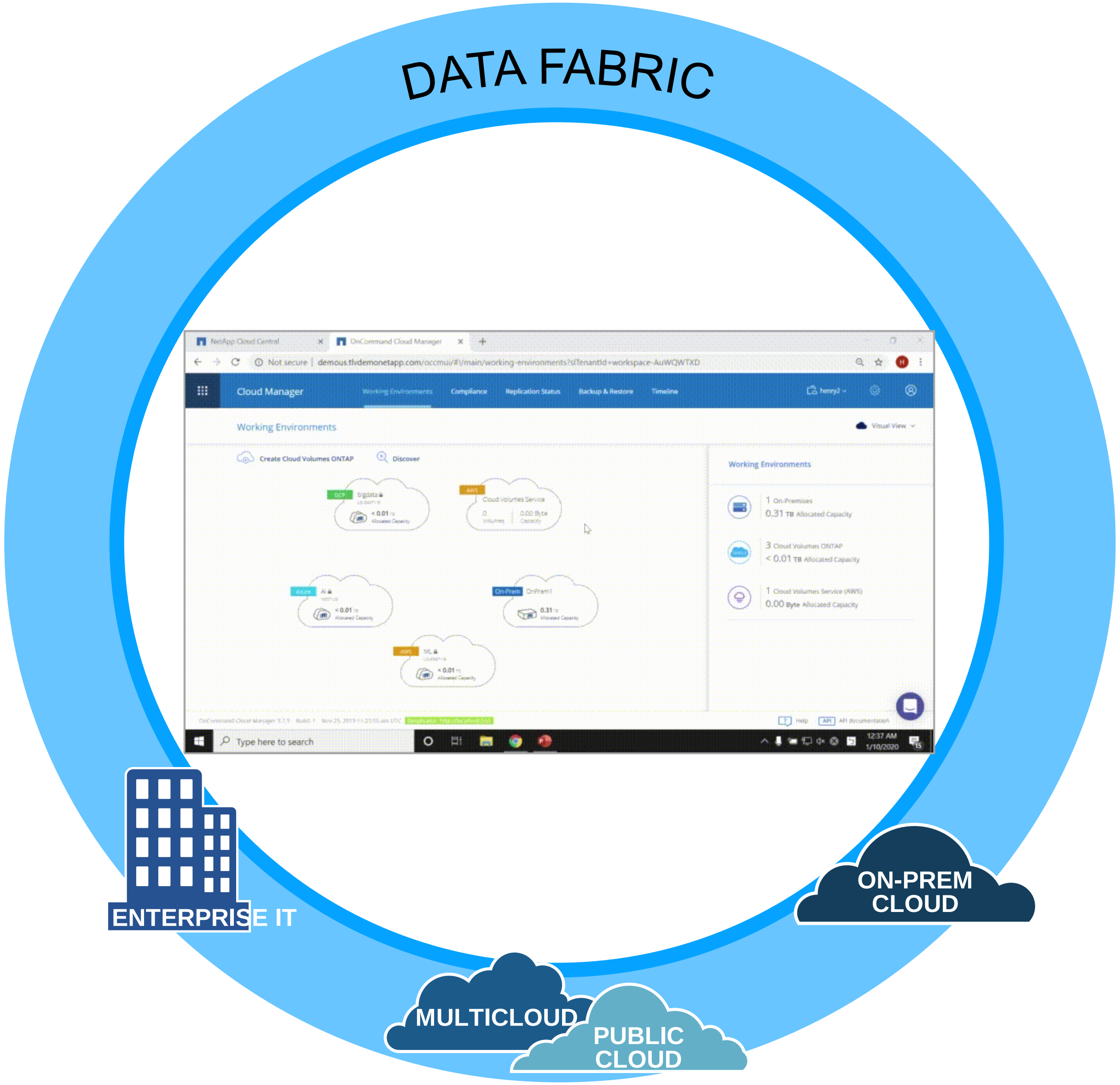
2490

2020
- FAS500f
- SnapMirror Business Continuity
- S3 in ONTAP
- SolidFire Software-Defined
- NFSv4.2
- FlexCache SMB Support
- IPsec In-Flight Data Encryption
- AI Control Plane
- Azure NetApp Files (ANF) Cross-Region Replication
- Azure NetApp Files (ANF) Backup and Restore
- Virtual Desktop Service/Virtual Desktop Managed Service (VDS/VDMS) (CloudJumper Acquisition)
- Global File Cache (GFC) (Talon Acquisition)
- Spot Acquisition, and later in the year, added Spot Storage
- Cloud Backup and Restore for both cloud and on-premises
- Cloud Compliance for both cloud and on-premises
- Astra, K8s Application Lifecycle Management
- Cloud Volume Service (CVS) Software-Defined
- Cloud Volume ONTAP (CVO) Storage VM’s
- Astra
- Cloud Manager SaaS
  - New K8s
  - New Compute (Spot Integration)
  - New Monitoring (Cloud Insights Integration)
  - SnapCenter Integration
  - Active IQ Integration
  - Global File Cache (GFC) Integration

我們的目標 – 建造您的 Data Farbic

運用我們豐富的以資料為中心的軟體創新服務，以協助客戶在混合雲世界中蓬勃發展

讓您可以自由地將資料放入可提升業務的應用程式中



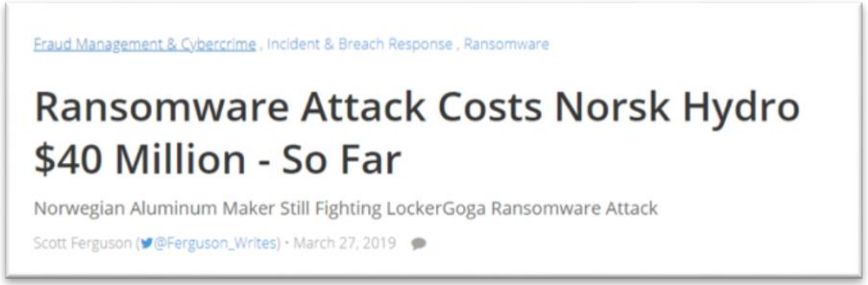
NetApp 是....

以雲為主導、資料為中心的
軟體公司

Ransomware is a threat to everyone.

勒索病毒對每個人都是威脅

勒索病毒一直發生在你我周遭....

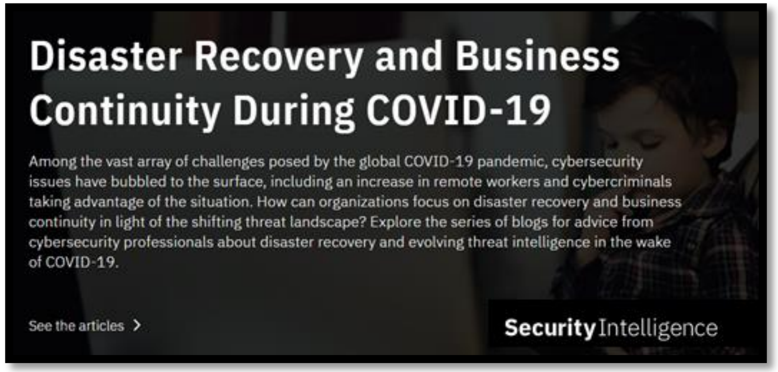


Fraud Management & Cybercrime , Incident & Breach Response , Ransomware

Ransomware Attack Costs Norsk Hydro $40 Million - So Far

Norwegian Aluminum Maker Still Fighting LockerGoga Ransomware Attack

Scott Ferguson (@Ferguson_Writes) • March 27, 2019

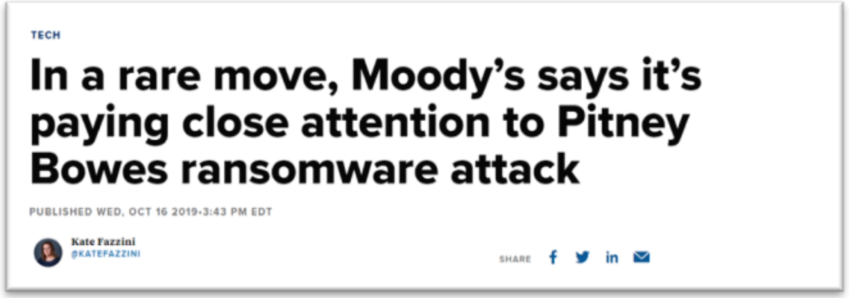


Disaster Recovery and Business Continuity During COVID-19

Among the vast array of challenges posed by the global COVID-19 pandemic, cybersecurity issues have bubbled to the surface, including an increase in remote workers and cybercriminals taking advantage of the situation. How can organizations focus on disaster recovery and business continuity in light of the shifting threat landscape? Explore the series of blogs for advice from cybersecurity professionals about disaster recovery and evolving threat intelligence in the wake of COVID-19.

See the articles >

SecurityIntelligence



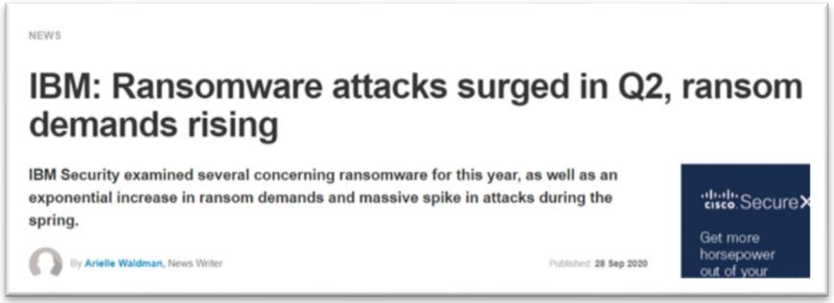
TECH

In a rare move, Moody's says it's paying close attention to Pitney Bowes ransomware attack

PUBLISHED WED, OCT 16 2019•3:43 PM EDT

Kate Fazzini
@KATEFAZZINI

SHARE



NEWS

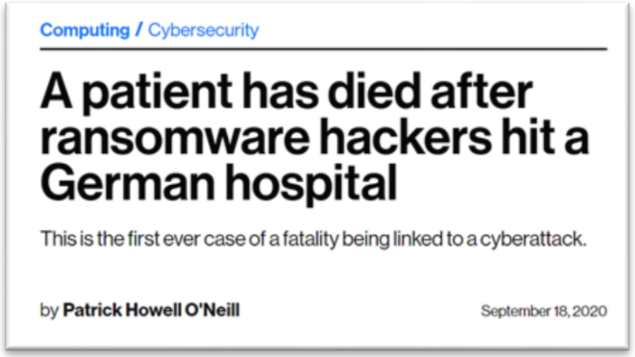
IBM: Ransomware attacks surged in Q2, ransom demands rising

IBM Security examined several concerning ransomware for this year, as well as an exponential increase in ransom demands and massive spike in attacks during the spring.

By Arielle Waldman, News Writer

Published: 28 Sep 2020

cisco SecureX
Get more horsepower out of your



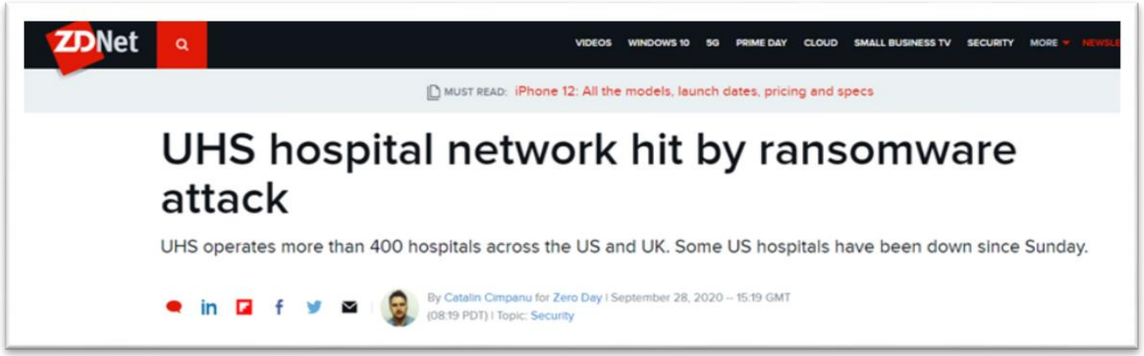
Computing / Cybersecurity

A patient has died after ransomware hackers hit a German hospital

This is the first ever case of a fatality being linked to a cyberattack.

by **Patrick Howell O'Neill**

September 18, 2020



ZDNet

VIDEOS WINDOWS 10 5G PRIME DAY CLOUD SMALL BUSINESS TV SECURITY MORE NEWSLE

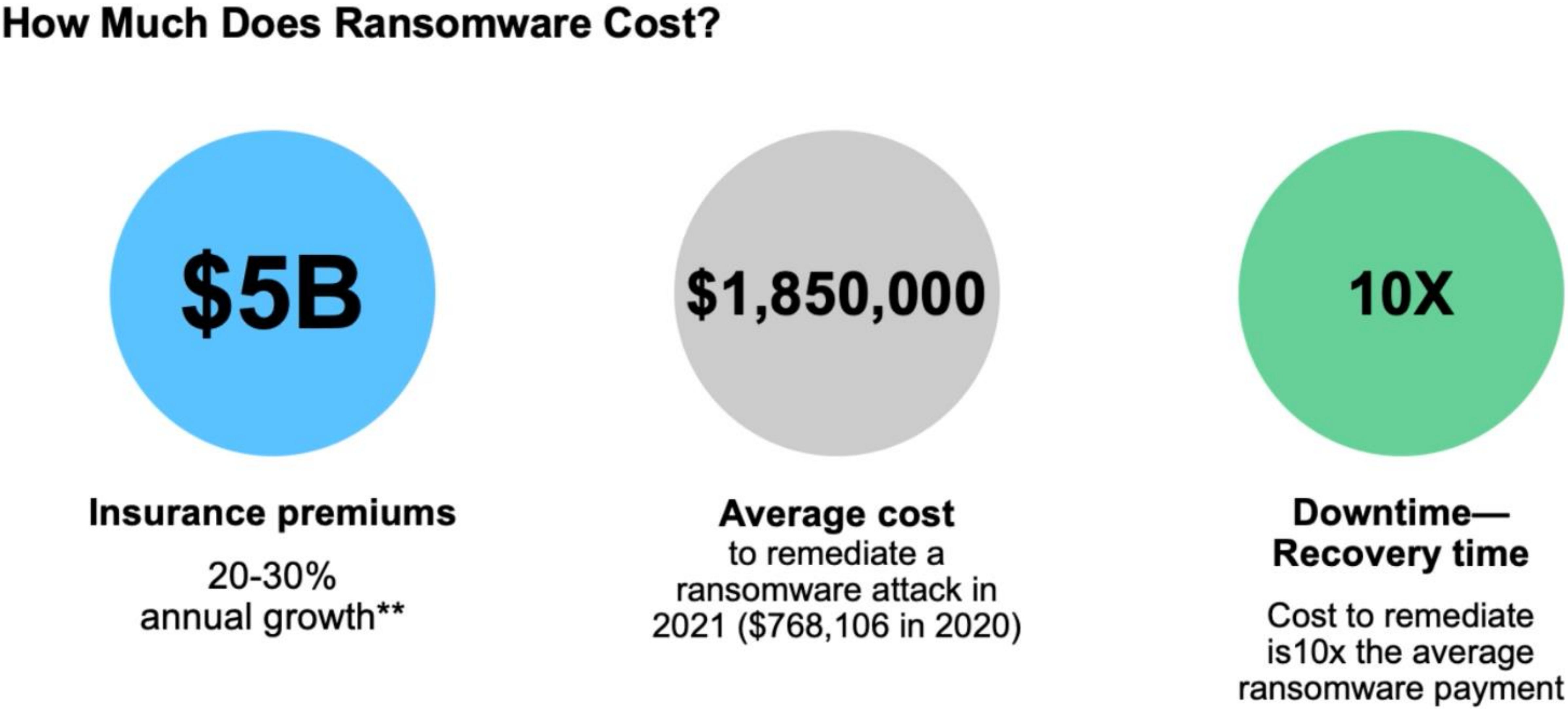
MUST READ: iPhone 12: All the models, launch dates, pricing and specs

UHS hospital network hit by ransomware attack

UHS operates more than 400 hospitals across the US and UK. Some US hospitals have been down since Sunday.

By Catalin Cimpanu for Zero Day | September 28, 2020 -- 15:19 GMT (08:19 PDT) | Topic: Security

勒索病毒造成企業巨大的損失....



How Much Does Ransomware Cost?

$5B

Insurance premiums

20-30%
annual growth**

$1,850,000

Average cost
to remediate a
ransomware attack in
2021 ($768,106 in 2020)

10X

Downtime—
Recovery time

Cost to remediate
is10x the average
ransomware payment

*Sophos report survey data of 5,400 IT manager on “The State Of Ransomware 2021” Average cost was for U.S. companies.
** Standard and Poor’s report.

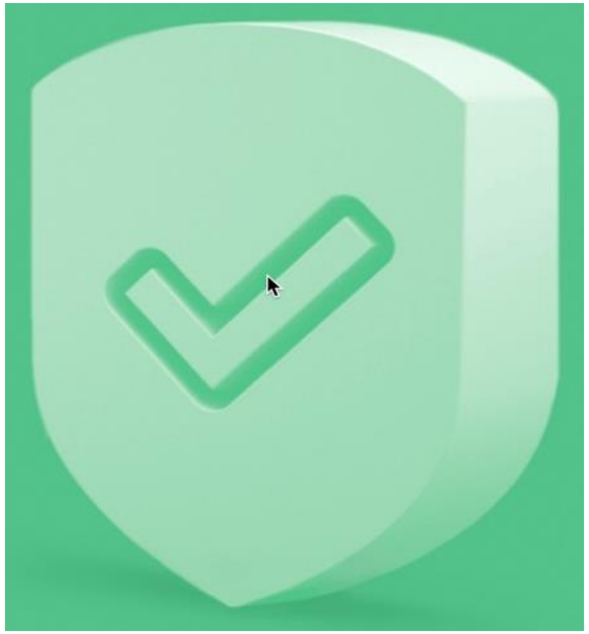
NetApp 企業資料保護 End-to-End 完整解決方案

輕鬆達成建構、維運、擺脫勒索軟體威脅

1. 沒有疊床架屋的複雜架構, 不需購買層層堆疊的設備
2. 軟體服務式的主動通知, 告警及防護處置
3. 閃電般秒級的資料還原, 降低Downtime及企業損失
4. 符合法規遵循的最高標準, 資料保護無後顧之憂

超高可用度儲存設備硬體

符合最高規格加密認證



主動式勒索軟體保護及防護

給您業界最高可用性 – NetApp 持續榮獲第三方的肯定
無論Block, File或是Object 存取應用，NetApp都可以給您優於業界最高級別的穩定可靠度

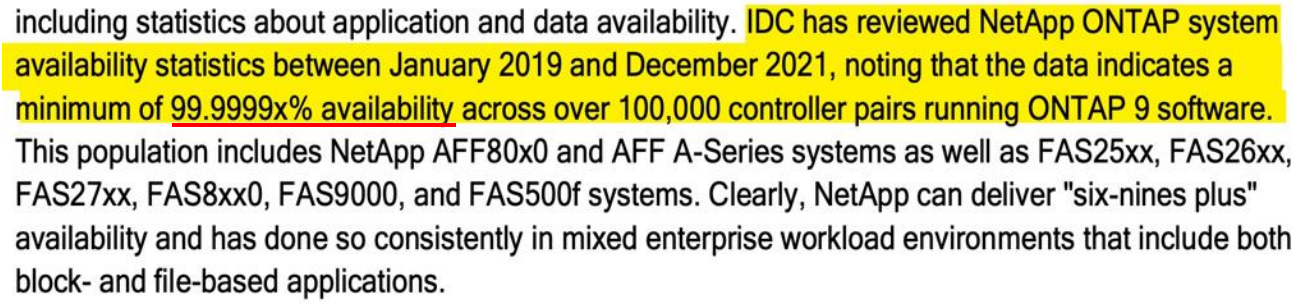
IDC白皮書：滿足企業數位轉型的高可用性要要求

White Paper

Meeting the High Availability Requirements in Digitally Transformed Enterprises

Sponsored by: NetApp

Eric Burgener
March 2022



including statistics about application and data availability. IDC has reviewed NetApp ONTAP system availability statistics between January 2019 and December 2021, noting that the data indicates a minimum of 99.9999x% availability across over 100,000 controller pairs running ONTAP 9 software. This population includes NetApp AFF80x0 and AFF A-Series systems as well as FAS25xx, FAS26xx, FAS27xx, FAS8xx0, FAS9000, and FAS500f systems. Clearly, NetApp can deliver "six-nines plus" availability and has done so consistently in mixed enterprise workload environments that include both block- and file-based applications.

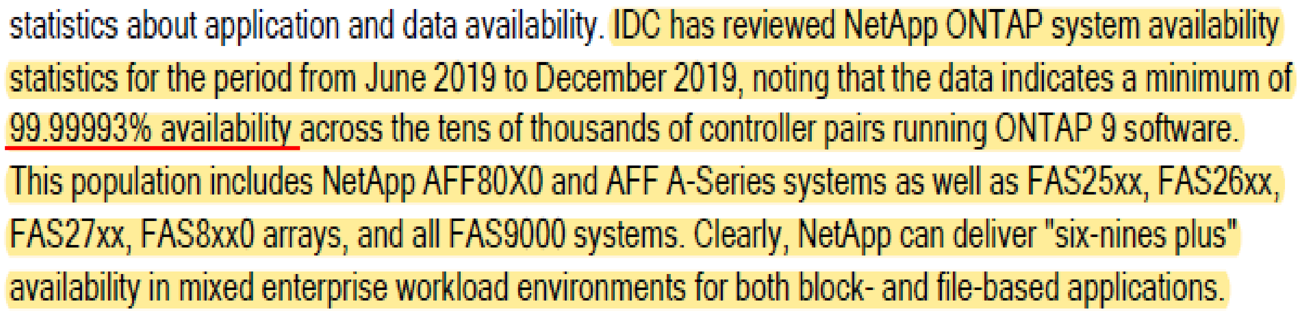
IDC White Paper《 Meeting the High Availability Requirements in Digitally Transformed Enterprises 》，文件編號 US48442021 ，2022 年 3 月

White Paper

Evolving Availability Requirements Demand More Than Just a Resilient Storage Infrastructure

Sponsored by: NetApp

Eric Burgener
February 2020



statistics about application and data availability. IDC has reviewed NetApp ONTAP system availability statistics for the period from June 2019 to December 2019, noting that the data indicates a minimum of 99.99993% availability across the tens of thousands of controller pairs running ONTAP 9 software. This population includes NetApp AFF80X0 and AFF A-Series systems as well as FAS25xx, FAS26xx, FAS27xx, FAS8xx0 arrays, and all FAS9000 systems. Clearly, NetApp can deliver "six-nines plus" availability in mixed enterprise workload environments for both block- and file-based applications.

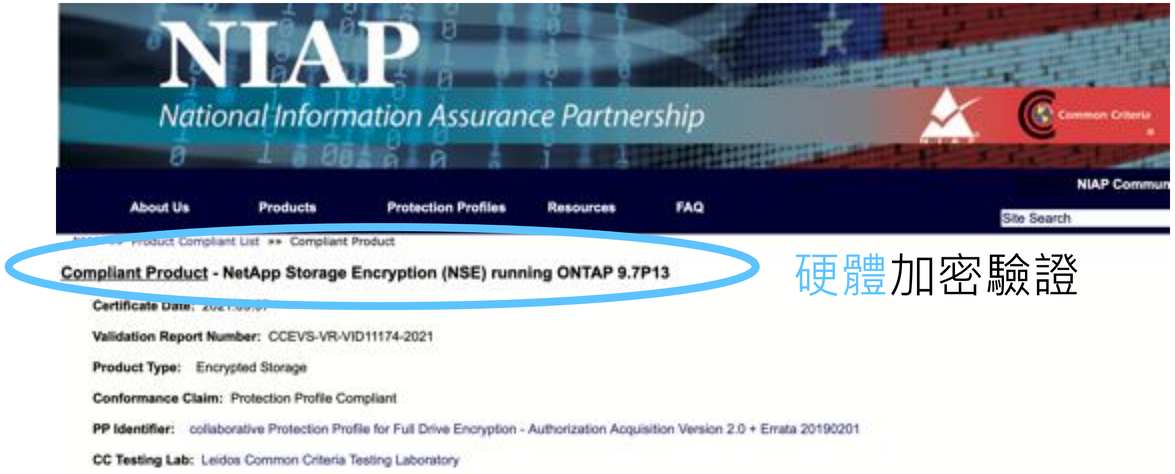
IDC White Paper《 Evolving Availability Requirements Demand More Than Just a Resilient Storage Infrastructure 》，文件編號 US46076020，2020 年 2 月

符合最高規格加密認證

NetApp ONTAP 成為首個通過 *美國國家安全局* (NSA) 安全和加密驗證的企業儲存平台

- What is CSfC?
  - 由美國國家安全局 (NSA) 領導的網路安全計劃，CSfC 是該組織商業網路安全戰略的關鍵組成部分。
  - CSfC 驗證商業 IT 產品是否滿足最高級別的嚴格加密標準以及軟硬體解決方案的嚴格安全要求。
  - NSA 已開始建議託管機密或絕密數據的聯邦機構使用已經過 CSfC 驗證的儲存解決方案。

- 通過此 CSfC 驗證，NetApp ONTAP 可幫助企業用戶：
  - **資料儲存信賴可靠** – 適合儲存機密和最高機密級別的數據資料
  - **節省時間** – 數據資料的搬移和儲存都是在已經過驗證的安全解決方案內, 可降低資料稽核及限制取用流程所需額外時間
  - **節省成本** – 可減少監控、降低物理數據傳輸和運輸成本
  - **零信任資訊安全架構基礎** – 同時在硬體和軟體層保護數據，可強化具備網路彈性且以數據為中心的安全性


NIAP
National Information Assurance Partnership
Common Criteria
NIAP Commun
About Us
Products
Protection Profiles
Resources
FAQ
Site Search
NIAP » Product Compliant List » Compliant Product

Compliant Product - NetApp Storage Encryption (NSE) running ONTAP 9.7P13

Certificate Date: [illegible]

Validation Report Number: CCEVS-VR-VID11174-2021

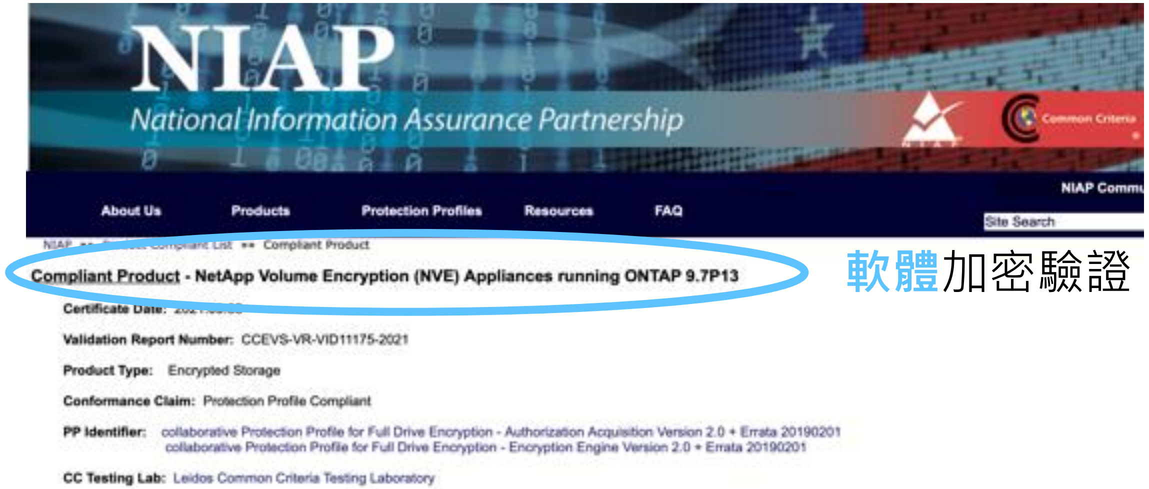
Product Type: Encrypted Storage

Conformance Claim: Protection Profile Compliant

PP Identifier: collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition Version 2.0 + Errata 20190201

CC Testing Lab: Leidos Common Criteria Testing Laboratory

硬體加密驗證


NIAP
National Information Assurance Partnership
Common Criteria
NIAP Commu
About Us
Products
Protection Profiles
Resources
FAQ
Site Search
NIAP » Product Compliant List » Compliant Product

Compliant Product - NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13

Certificate Date: [illegible]

Validation Report Number: CCEVS-VR-VID11175-2021

Product Type: Encrypted Storage

Conformance Claim: Protection Profile Compliant

PP Identifier: collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition Version 2.0 + Errata 20190201
collaborative Protection Profile for Full Drive Encryption - Encryption Engine Version 2.0 + Errata 20190201

CC Testing Lab: Leidos Common Criteria Testing Laboratory

軟體加密驗證

NetApp

https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Components-List/
https://www.netapp.com/newsroom/press-releases/news-rel-20211215-870245/

Gartner’s 對下一世代儲存設備的要求：Cyber Storage

不用擔心!!NetApp全方位守護您的企業資產

Detect

Protect

Respond

Recover

By 2025, 40% of all enterprises will require storage products to have integrated ransomware defense mechanisms, up from 10% in 2021

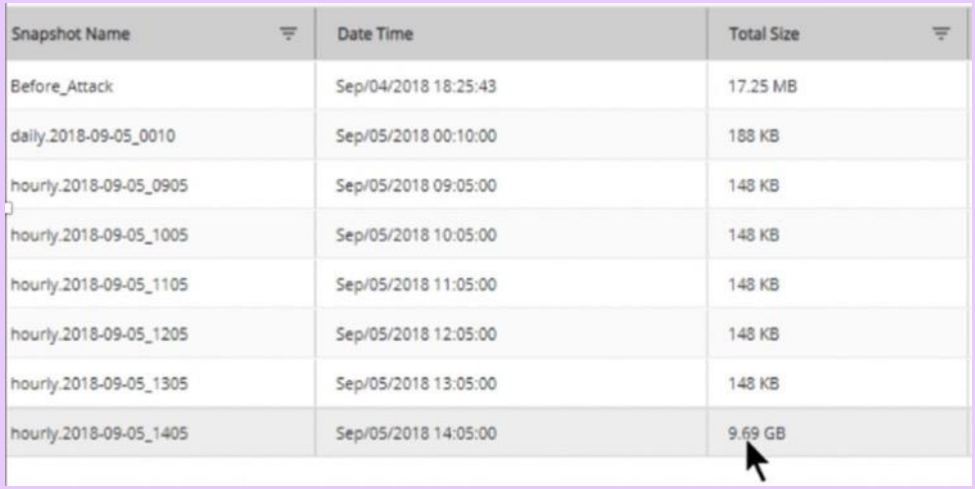
NetApp Solution for Ransomware

協助企業偵測異常狀態

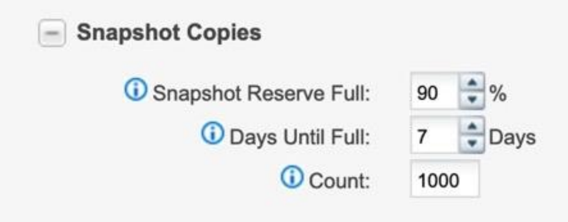
Detect

直覺式異常指標偵測

- NetApp Snapshot™ copy rate of change as a key indicator
- Decrease in storage efficiencies (dedupe and compression)
  - **NetApp Active IQ® Unified Manager now has an efficiency loss alert in ONTAP 9.10.1**



Snapshot Name	Date Time	Total Size
Before_Attack	Sep/04/2018 18:25:43	17.25 MB
daily.2018-09-05_0010	Sep/05/2018 00:10:00	188 KB
hourly.2018-09-05_0905	Sep/05/2018 09:05:00	148 KB
hourly.2018-09-05_1005	Sep/05/2018 10:05:00	148 KB
hourly.2018-09-05_1105	Sep/05/2018 11:05:00	148 KB
hourly.2018-09-05_1205	Sep/05/2018 12:05:00	148 KB
hourly.2018-09-05_1305	Sep/05/2018 13:05:00	148 KB
hourly.2018-09-05_1405	Sep/05/2018 14:05:00	9.69 GB

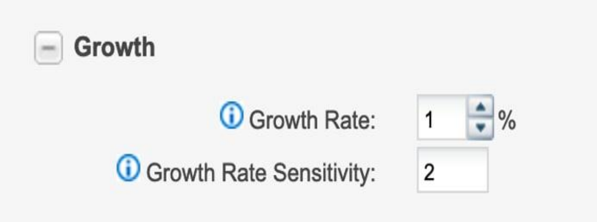


Snapshot Copies

Snapshot Reserve Full: 90 %

Days Until Full: 7 Days

Count: 1000



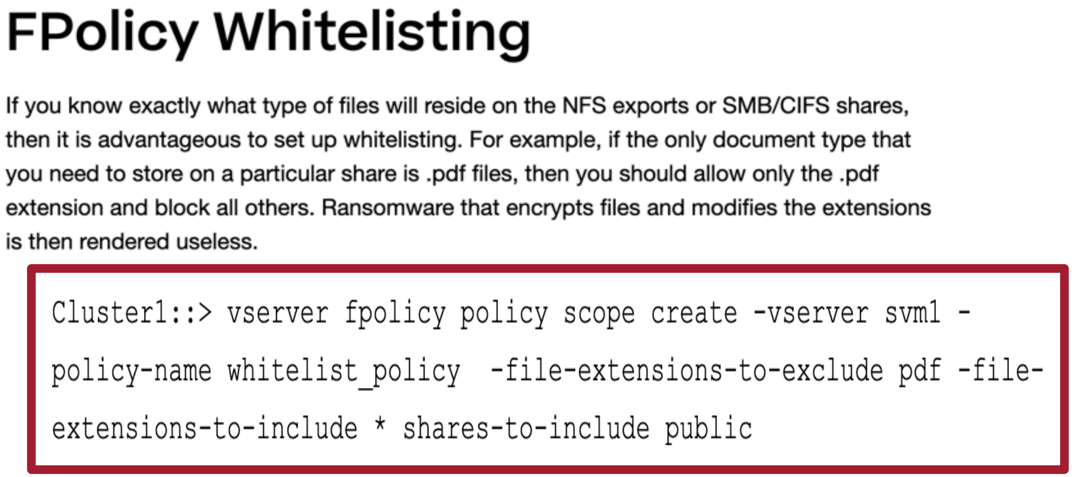
Growth

Growth Rate: 1 %

Growth Rate Sensitivity: 2

NetApp Solution for Ransomware

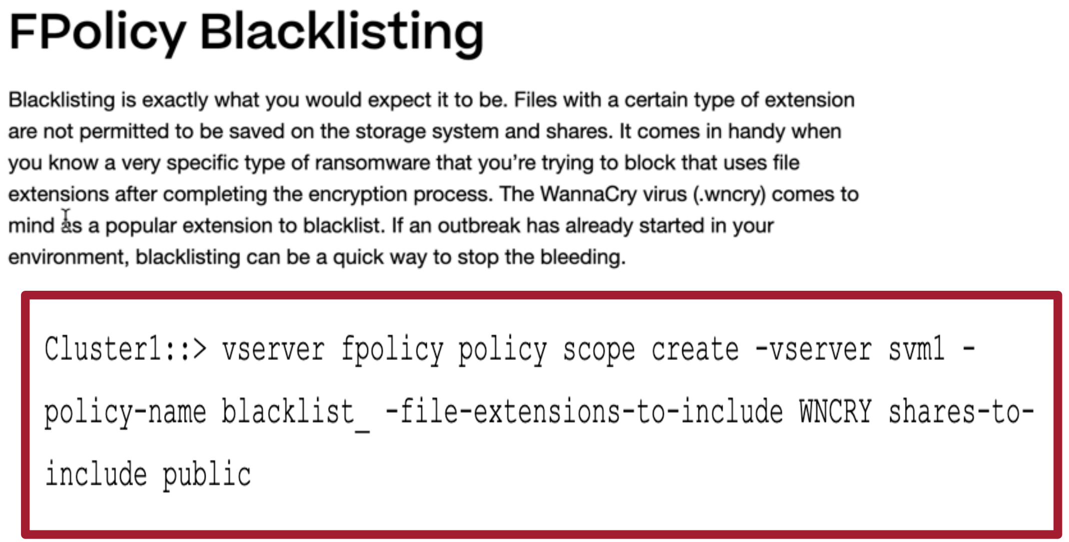
協助企業阻斷異常存取 (設定黑白名單及整合)



FPolicy Whitelisting

If you know exactly what type of files will reside on the NFS exports or SMB/CIFS shares, then it is advantageous to set up whitelisting. For example, if the only document type that you need to store on a particular share is .pdf files, then you should allow only the .pdf extension and block all others. Ransomware that encrypts files and modifies the extensions is then rendered useless.

```
Cluster1::> vserver fpolicy policy scope create -vserver svm1 -
policy-name whitelist_policy  -file-extensions-to-exclude pdf -file-
extensions-to-include * shares-to-include public
```



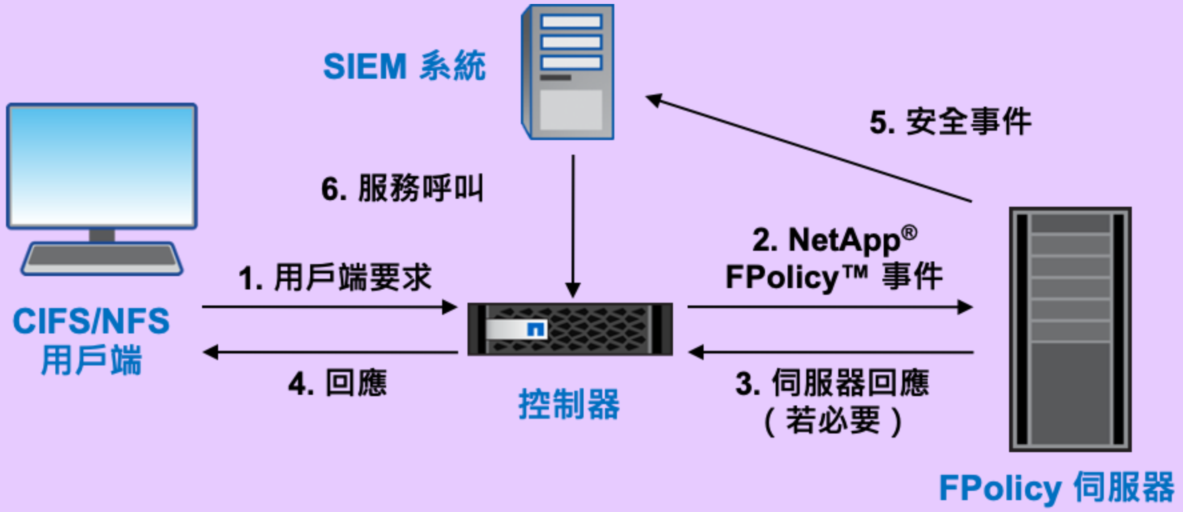
FPolicy Blacklisting

Blacklisting is exactly what you would expect it to be. Files with a certain type of extension are not permitted to be saved on the storage system and shares. It comes in handy when you know a very specific type of ransomware that you're trying to block that uses file extensions after completing the encryption process. The WannaCry virus (.wncry) comes to mind as a popular extension to blacklist. If an outbreak has already started in your environment, blacklisting can be a quick way to stop the bleeding.

```
Cluster1::> vserver fpolicy policy scope create -vserver svm1 -
policy-name blacklist_ -file-extensions-to-include WNCRY shares-to-
include public
```

NetApp® FPolicy™ 整合第三方合作夥伴：

- 以檔案與使用者行為分析 (UBA) 為基礎，發送事件通知給第三方合作夥伴
- 安全資訊與事件管理 (SIEM) 整合



NetApp Solution for Ransomware

主動協助企業偵測異常及啟動資料保護

Detect

Protect

NetApp® ONTAP® Onbox anti-ransomware

- Automatic detection of ransomware in 9.10.1
- Leverages volume workload activity and entropy

NetApp Cloud Insights / Cloud Secure

- Monitors files that access NetApp file systems
- Cloud Secure leverages UEBA to detect and stop attacks

NetApp Solution for Ransomware

主動協助企業偵測異常, 啟動資料保護並觸發通知

ONTAP Anti-ransomware – 儲存設備自動偵測

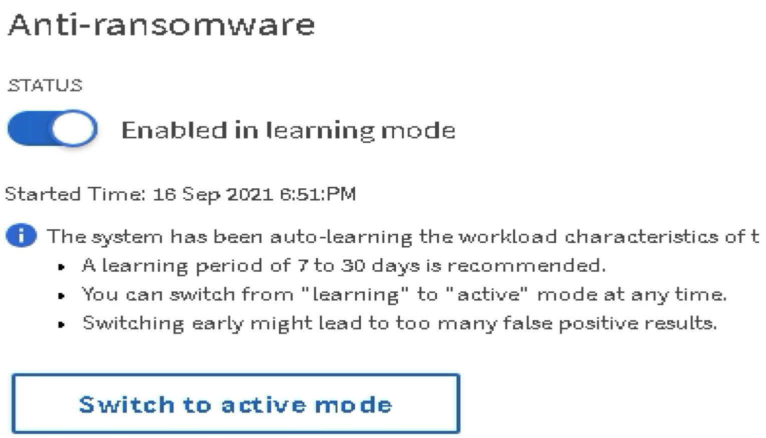
Available in NetApp® ONTAP® 9.10.1 for NAS

NetApp Onbox ML analytics engine leverages volume file activity and data entropy

Automatically takes NetApp Snapshot™ copy

Negligible performance impact

Additional layer of detection and ransomware protection



Anti-ransomware

STATUS

Enabled in learning mode

Started Time: 16 Sep 2021 6:51:PM

The system has been auto-learning the workload characteristics of t

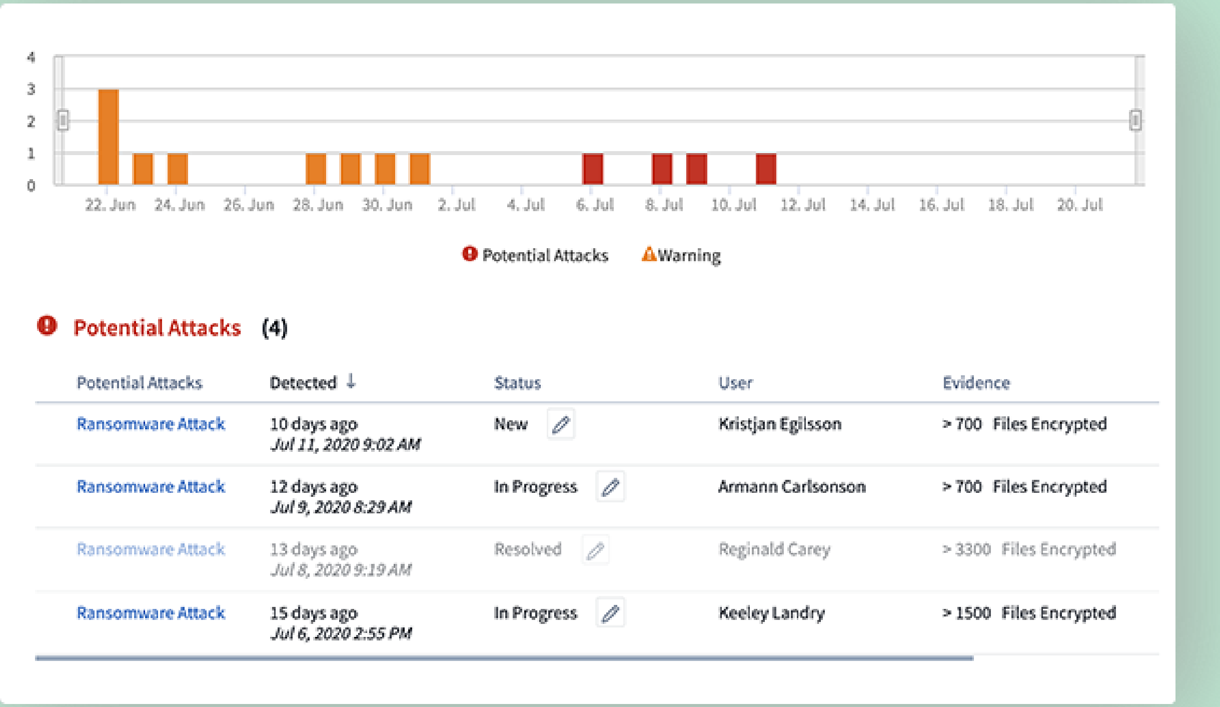
- A learning period of 7 to 30 days is recommended.
- You can switch from "learning" to "active" mode at any time.
- Switching early might lead to too many false positive results.

Cloud Secure – 雲端服務 – 使用者異常行為

UBA leveraging NetApp Cloud Secure

Detects abnormal change in user activity

Analyzes abnormal behavior patterns to determine type of threat



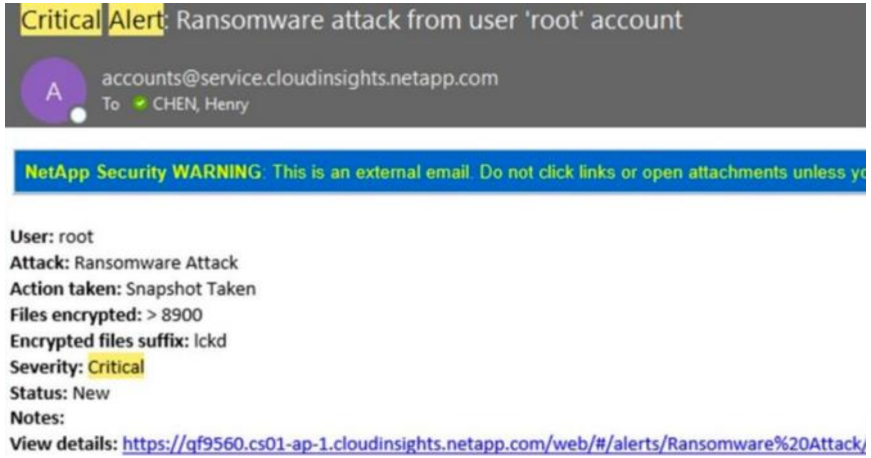
Potential Attacks (4)

Potential Attacks	Detected ↓	Status	User	Evidence
Ransomware Attack	10 days ago Jul 11, 2020 9:02 AM	New	Kristjan Egilsson	> 700 Files Encrypted
Ransomware Attack	12 days ago Jul 9, 2020 8:29 AM	In Progress	Armann Carlsonson	> 700 Files Encrypted
Ransomware Attack	13 days ago Jul 8, 2020 9:19 AM	Resolved	Reginald Carey	> 3300 Files Encrypted
Ransomware Attack	15 days ago Jul 6, 2020 2:55 PM	In Progress	Keeley Landry	> 1500 Files Encrypted

NetApp Solution for Ransomware

協助企業偵測異常後的主動處置

Respond



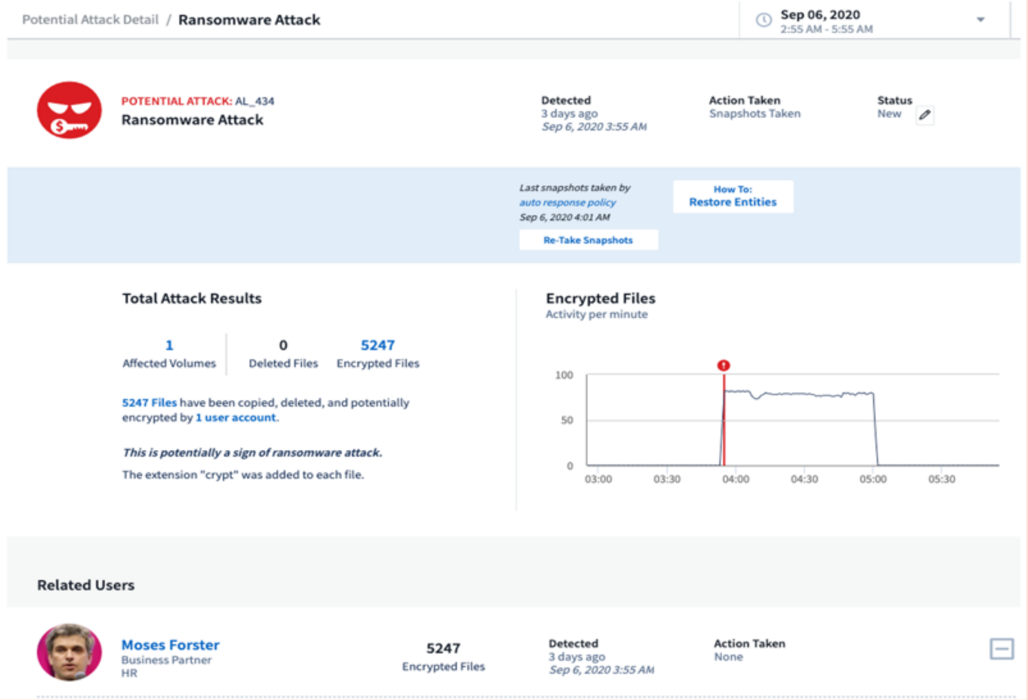
Critical Alert: Ransomware attack from user 'root' account

accounts@service.cloudinsights.netapp.com
To CHEN, Henry

NetApp Security WARNING: This is an external email. Do not click links or open attachments unless yo

User: root
Attack: Ransomware Attack
Action taken: Snapshot Taken
Files encrypted: > 8900
Encrypted files suffix: lckd
Severity: Critical
Status: New
Notes:
View details: https://qf9560.cs01-ap-1.cloudinsights.netapp.com/web/#/alerts/Ransomware%20Attack/

- 一但勒索威脅被識別, NetApp® Snapshot™ 會立即被觸發



Potential Attack Detail / Ransomware Attack

Sep 06, 2020
2:55 AM - 5:55 AM

POTENTIAL ATTACK: AL_434
Ransomware Attack

Detected
3 days ago
Sep 6, 2020 3:55 AM

Action Taken
Snapshots Taken

Status
New

Last snapshots taken by
auto response policy
Sep 6, 2020 4:01 AM

Total Attack Results

1	0	5247
Affected Volumes	Deleted Files	Encrypted Files

5247 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of ransomware attack.

The extension "crypt" was added to each file.

Encrypted Files
Activity per minute

Related Users

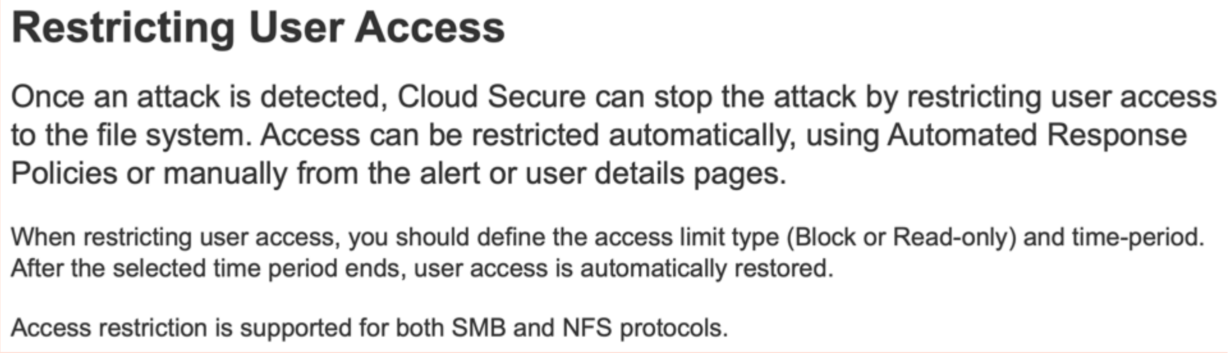
Moses Forster
Business Partner
HR

5247
Encrypted Files

Detected
3 days ago
Sep 6, 2020 3:55 AM

Action Taken
None

- 限制遭受感染的人員存取



Restricting User Access

Once an attack is detected, Cloud Secure can stop the attack by restricting user access to the file system. Access can be restricted automatically, using Automated Response Policies or manually from the alert or user details pages.

When restricting user access, you should define the access limit type (Block or Read-only) and time-period. After the selected time period ends, user access is automatically restored.

Access restriction is supported for both SMB and NFS protocols.

NetApp Solution for Ransomware

偵測到勒索軟體後的資料補救措施

- 儲存設備資料復原：
  - 找出狀態良好的備份或 NetApp® Snapshot™ 快照複本
  - 從乾淨的備份或 Snapshot 快照複本中還原資料

1. 藉由 Snapshot 秒級還原

   快速排除問題 (不論資料有多大)
2. 想照就照 自動排程

   效能影響最小
3. SnapShot 唯讀保護

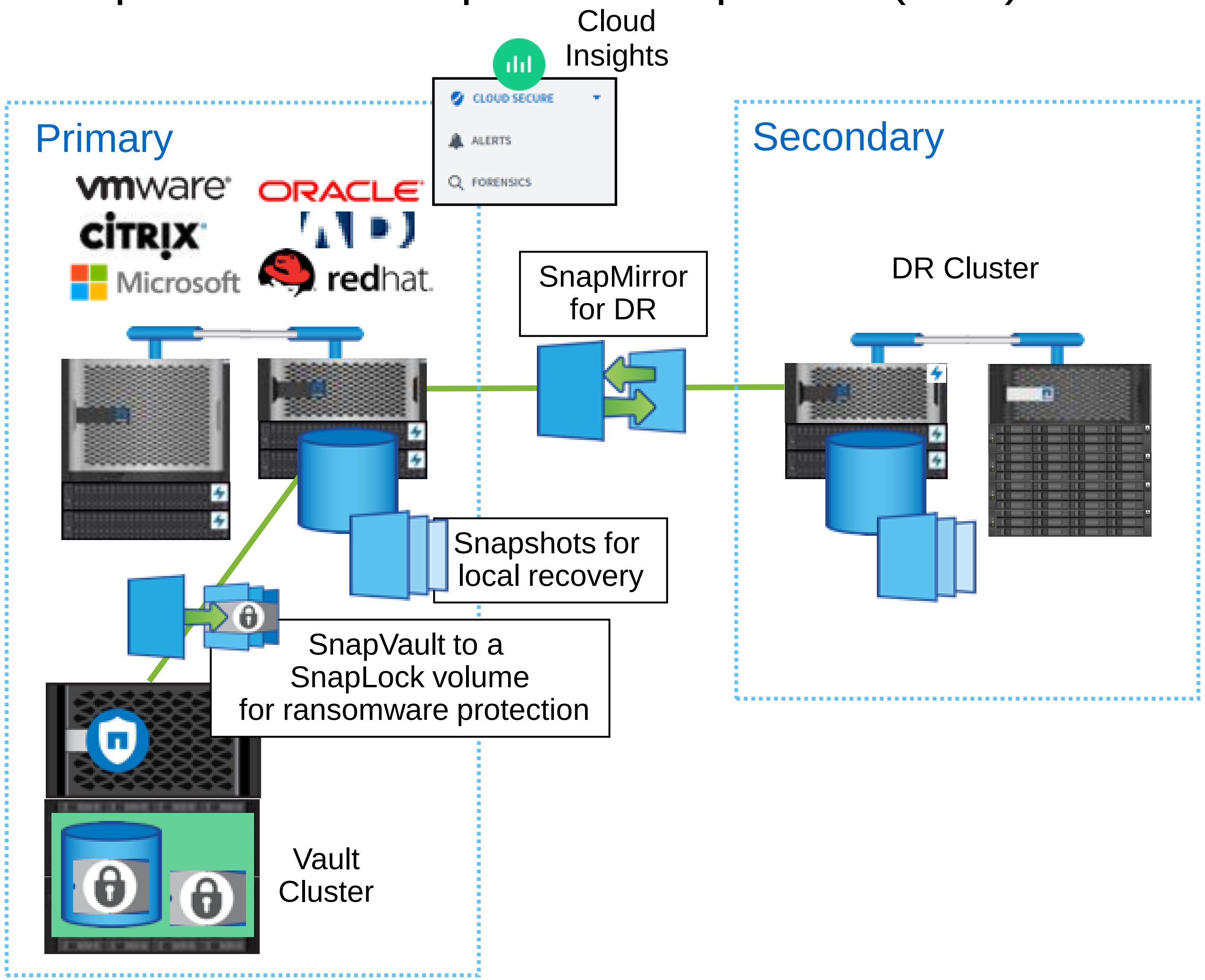
   多一道可靠防線 避免遭受感染
4. 應用服務整合最多(SnapCenter)

   虛擬化、應用程式、資料庫
5. 不怕萬一(SnapMirror/SnapVault)

   快照帶著走，雲/地端任您選

將您的快照保護存放至不可變更的儲存設備 – 比AirGap更安全完整的解決方案

SnapVault with SnapLock Compliance (SLC)



Cloud Insights

Primary

Secondary

SnapMirror for DR

DR Cluster

Snapshots for local recovery

SnapVault to a SnapLock volume for ransomware protection

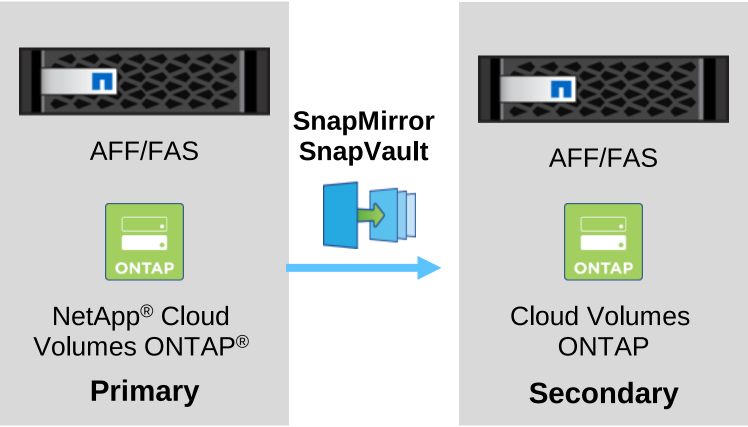
Vault Cluster

- For Local Recovery - Continue to use Snapshots
- For Disaster Recovery - Continue to use SnapMirror to a secondary data center
- For Ransomware Protection - Use SnapVault and SnapLock to create <u>immutable</u> AND <u>indelible</u> backups
- Add a Vault Cluster at the primary or secondary data center
  - Create an SLC storage tier on the Vault Cluster
  - Create an SLC volume on the SLC storage tier
  - Create SLC retention, SnapVault relationship, rule, and schedule
  - Execute SnapVault to the SLC volume
- SnapVault backups to SnapLock Compliance volumes are essentially “air gapped”
  - Are indelible - can’t be deleted
  - Are still online for quick recovery

NetApp 資料保護的解決方案 比您想像的多更多

SnapCenter 滿足企業應用程式資料一致性的資料保護

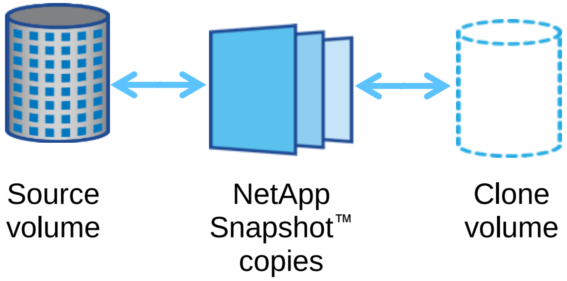
On-premises backup and recovery of NetApp ONTAP platforms only



Backup copies

Analytics copies

Test and Dev copies



NetApp supported

- Exchange
- ORACLE DATABASE
- Microsoft SQL Server
- SAP HANA
- Windows
- vmware

Custom supported

- mongoDB
- IBM DB2
- MySQL
- SAP MaxDB The SAP Database
- PostgreSQL
- SAP ASE Sybase

COMMVAULT CLEONDRIS VERITAS veeam CATALOGIC SOFTWARE rubrik

Integrated Application Backup Software

NetApp小學堂影片系列三：勒索病毒的預防及保護

https://www.youtube.com/watch?v=iDkFpUN4HdI&t=119s

NetApp

NetApp 小學堂

勒索病毒的預防及保護

蘇子婷 Ting Su

NetApp 產品技術顧問

© 2021 NetApp, Inc. All rights reserved. — NETAPP CONFIDENTIAL —

Key Takeaways

- NetApp 以雲為主導、資料為中心的軟體公司
- NetApp 提供最高級別的資料保護解決方案
  - 業界最高 99.99993 高可靠度
  - 符合NSA最高級別嚴格加密標準
  - 提供設定簡單, 無硬體堆疊的防範勒索威脅整合方案

Thank you !